[0248] A wide variety of devices may be used to implement the data memories discussed herein. For example, a data memory may comprise flash memory, one-time-programmable (OTP) memory or other types of data storage devices.

[0249] In summary, the invention described herein generally relates to an improved authentication system and method. While certain exemplary embodiments have been described above in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not restrictive of the broad invention. In particular, it should be recognized that the teachings of the invention apply to a wide variety of systems and processes. It will thus be recognized that various modifications may be made to the illustrated and other embodiments of the invention described above, without departing from the broad inventive scope thereof. In view of the above it will be understood that the invention is not limited to the particular embodiments or arrangements disclosed, but is rather intended to cover any changes, adaptations or modifications which are within the scope and spirit of the invention as defined by the appended claims.

What is claimed is:

1. An authentication method comprising:

receiving authentication data at an input device;

cryptographically processing the authentication data at the input device;

transmitting the cryptographically processed authentication data to an access device;

processing the transmitted authentication data at the access device;

transmitting the processed authentication data to a service provider.

2. The method of claim 1 wherein cryptographically processing includes at least one of authenticating and encrypting.

3. The method of claim 1 wherein cryptographically processing comprises using a symmetric key provided by the access device.

4. The method of claim 1 wherein cryptographically processing comprises using a symmetric key injected into the input device during manufacture of the input device.

5. The method of claim 1 comprising establishing cryptographic link between the input device and the access device.

6. The method of claim 1 comprising performing asymmetric key operations between the input device and the access device.

7. The method of claim 1 comprising generating an asymmetric key pair within the input device.

8. The method of claim 1 comprising generating an asymmetric key pair within a security boundary of the input device.

9. The method of claim 1 wherein the authentication data is received within a security boundary of the input device.

10. The method of claim 1 wherein the input device comprises a sensor.

11. The method of claim 1 wherein the input device comprises a proximity authentication system.

12. The method of claim 1 wherein processing the transmitted authentication data comprising authenticating the transmitted authentication data.

13. The method of claim 1 wherein the service provider grants access to at least one service in response to the transmitted processed authentication data.

14. The method of claim 1 wherein the service provider enables access to a network in response to the transmitted processed authentication data.

15. A secure data processing system comprising:

an input device adapted to receive authentication data, cryptographically process the authentication data and transmit the cryptographically processed authentication data over a medium; and

an access device adapted to receive the transmitted authentication data, process the received authentication data and transmit the processed authentication data to a service provider.

16. The system of claim 15 wherein cryptographically process includes at least one of authenticating and encrypting.

17. The system of claim 15 wherein cryptographically process comprises using a symmetric key provided by the access device.

18. The system of claim 15 wherein cryptographically process comprises using a symmetric key injected into the input device during manufacture of the input device.

19. The system of claim 15 wherein the input device and the access device are adapted to establish a cryptographic link between the input device and the access device.

20. The system of claim 15 wherein the input device and the access device are adapted to perform asymmetric key operations between the input device and the access device.

21. The system of claim 15 wherein the input device is adapted to generate an asymmetric key pair.

22. The system of claim 15 wherein the input device is adapted to generate an asymmetric key pair within a security boundary of the input device.

23. The system of claim 15 wherein the authentication data is received within a security boundary of the input device.

24. The system of claim 15 wherein the input device comprises a sensor.

25. The system of claim 15 wherein the input device comprises a proximity authentication system.

26. The system of claim 15 wherein processing the transmitted authentication data comprising authenticating the transmitted authentication data.

27. The system of claim 15 wherein the service provider grants access to at least one service in response to the transmitted processed authentication data.

28. The system of claim 15 wherein the service provider enables access to a network in response to the transmitted processed authentication data.

* * * * *